

20040404 "136410260"

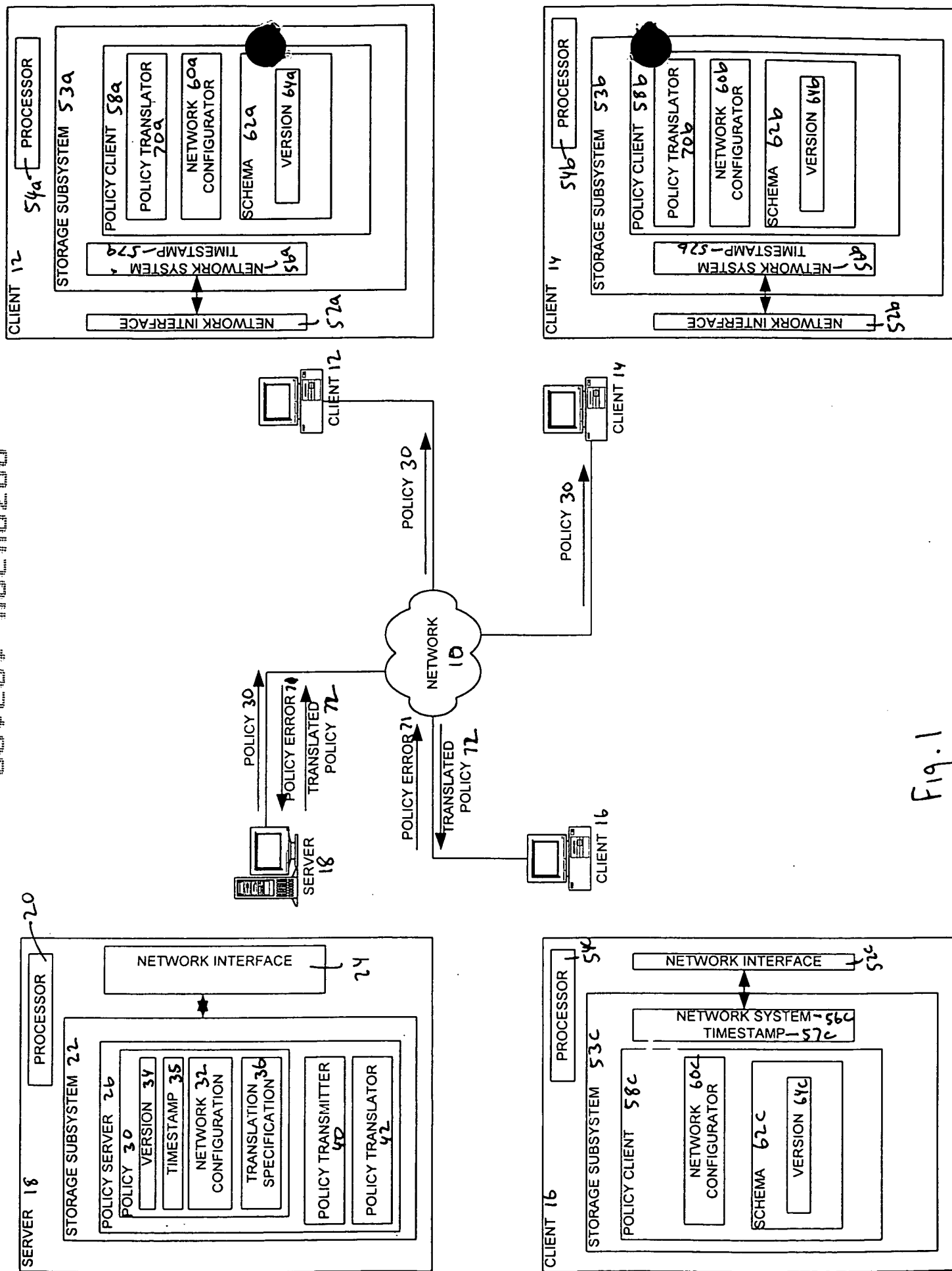


Fig. 1

DOCTYPE "public" NOTATION

// Policy that conforms to the newer schema (specifies Rjindael):

<?xml version="1.0"?>

<!DOCTYPE IPsecPolicyOnSystem PUBLIC "-//somestandard.org/IPsecPolicy/Version1.1">

<IPsecPolicyOnSystem timestamp="2000-9-30\_12:12:12"> 35  
 <IKEProposals>  
 90a 94a 96a 98a 92a  
 90b 94b 96b 98b 92b  
 </IKEProposals>  
</IPsecPolicyOnSystem> 30

Fig. 2

// DTD schema Version 1.1 for IPsec implementations that support the new  
// encryption algorithm called Rjindael:

<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>

<!--ATTLIST IKEProposal

162 id ID #REQUIRED 104 110 112  
168 CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST | Rjindael) #REQUIRED 120  
114 HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED 122  
116 GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED  
118 AuthenticationMethod (DSS\_Signatures | Preshared | RSA\_Signatures |  
RSA\_Encryption | Revised\_RSA\_Encryption | Kerberos) #REQUIRED 124

<!--ELEMENT IKEProposals (IKEProposal+)>

<!--ELEMENT IPsecPolicyOnSystem (IKEProposals)>

<!--ATTLIST IpsecPolicyOnSystem

timestamp CDATA #REQUIRED 126

>

Fig. 3

```
// DTD schema for version 1.0 IPsec policy implementations (doesn't
// include the new encryption algorithm called Rjindael):
<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>
<!-- ATTLIST IKEProposal
    id ID #REQUIRED
    CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST) #REQUIRED
    HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED
    GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED
    AuthenticationMethod (DSS_Signatures | Preshared | RSA_Signatures |
    RSA_Encryption | Revised_RSA_Encryption | Kerberos) #REQUIRED
-->

<!-- ELEMENT IKEProposals (IKEProposal+)>
<!-- ELEMENT IPsecPolicyOnSystem (IKEProposals)>
<!-- ATTLIST IPsecPolicyOnSystem
    timestamp CDATA #REQUIRED
-->
```

130

Fig. 4

// XSLT file to transform the above policy into a policy conforming to the older  
// schema. This transformation simply replaces attribute "Rjindael" with "3DES".

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This stylesheet replaces the CipherAlgorithm Rjindael with 3DES, for IKE
implementations that do not support Rjindael. -->
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes"/>
```

```
  <xsl:output doctype-public="//somestandard.org/IPsecPolicy/Version 1.0"/>
```

```
  <xsl:template match="/*">
    <xsl:element name="IPsecPolicyOnSystem">
      <xsl:copy-of select="@*" />
      <xsl:element name="IKEProposals">
        <xsl:apply-templates select="IKEProposals"/>
      </xsl:element>
    </xsl:element>
  </xsl:template>
```

```
  <xsl:template match="IKEProposals/IKEProposal">
```

```
    <xsl:element name="IKEProposal">
      <xsl:copy-of select="@*" />
```

```
      <xsl:if test="@CipherAlgorithm = 'Rjindael'">
```

```
        <xsl:attribute name="CipherAlgorithm">3DES</xsl:attribute>
```

```
      </xsl:if>
```

```
    </xsl:element>
```

```
  </xsl:template>
```

```
</xsl:stylesheet>
```

Fig. 5A

142 { 142a 142b 36

```
// Output resulting from applying the above transformation to the policy:

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE IPsecPolicyOnSystem PUBLIC "-//somestandard.org/IPsecPolicy/Version1.0">
<IPsecPolicyOnSystem timestamp="2000-9-30_12:12:12"> 150
  <IKEProposals>
    <IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/>
    <IKEProposal id="Proposal2" CipherAlgorithm="3DES" HashAlgorithm="SHA-1" GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/>
  </IKEProposals>
</IPsecPolicyOnSystem> 35
```

22

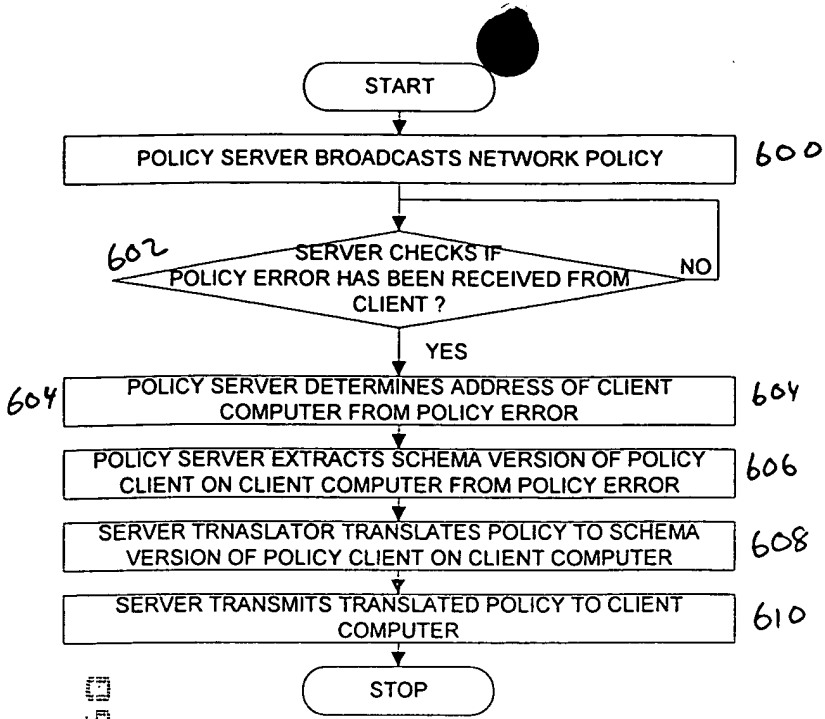


FIG. 6

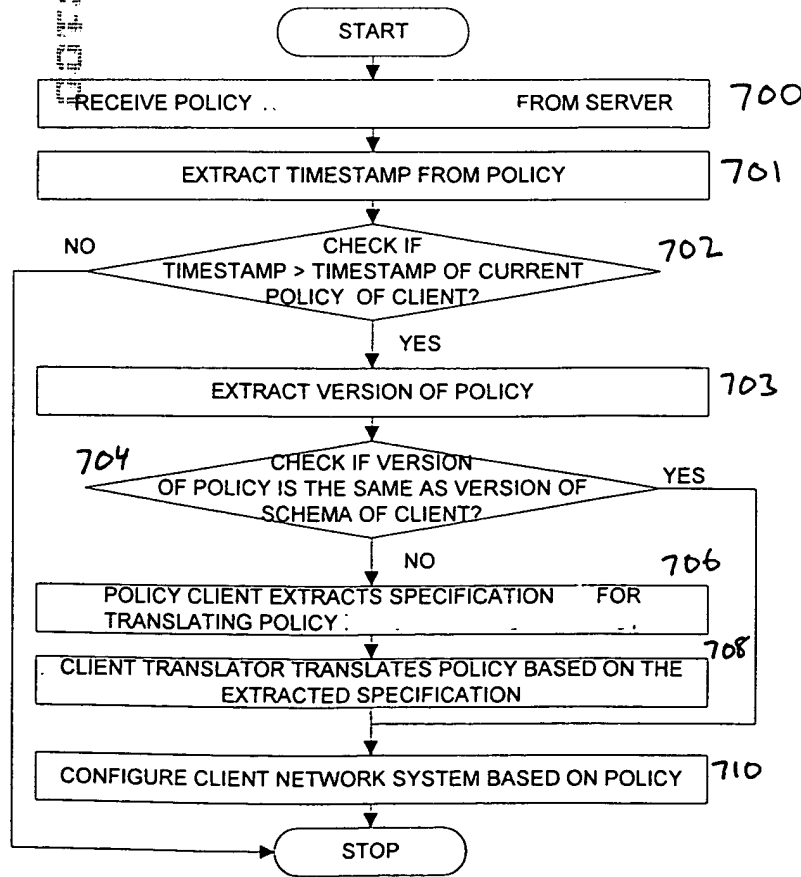


FIG. 7A

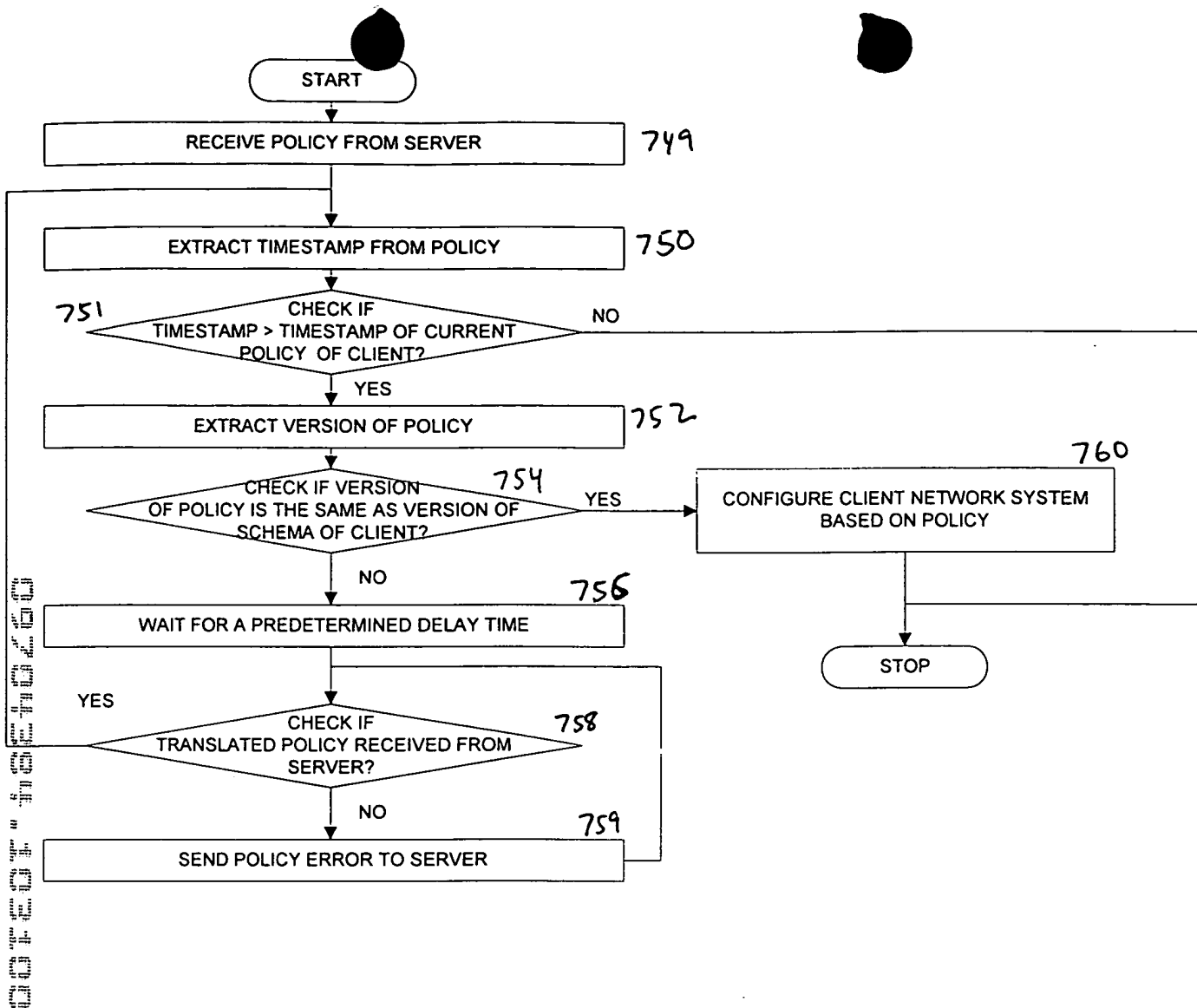


FIG. 7B